UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA, :

- v - : 05 Cr. 00004 (WHP)

WILLIAM GENOVESE, :

Defendant. :

----------X

DEFENDANT WILLIAM GENOVESE'S MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION TO DISMISS THE INDICTMENT

LEONARD F. JOY, ESQ.
The Legal Aid Society
Federal Defender Division,
SEAN HECKER, ESQ.
Attorneys for Defendant
WILLIAM GENOVESE
52 Duane Street, 10th Floor
New York, New York 10007
Tel.: (212) 417-8737

Also on the brief, *pro bono*:

DOMINIC PERELLA
Law Student
N.Y.U. School of Law

TO: DAVID E. KELLY, ESQ.
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007
Attn: ALEXANDER SOUTHWELL
Assistant United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA, :

- v - : 05 Cr. 00004 (WHP)

WILLIAM GENOVESE, :

Defendant. :

----------X

DEFENDANT WILLIAM GENOVESE'S MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION TO DISMISS THE INDICTMENT

INTRODUCTION

The defendant William Genovese, by and through his undersigned counsel, hereby moves to dismiss the sole count of the Indictment pursuant to Rule 12 of the Federal Rules of Criminal Procedure.

The government has charged Mr. Genovese with violating 18 U.S.C. § 1832(a), a section of the Economic Espionage Act ("EEA") which prohibits, among other things, the knowing downloading, distribution, or sale of "trade secrets." In this case, the government alleges that Mr. Genovese violated the statute by downloading and offering for sale on his website portions of the computer source code for two Microsoft Inc. ("Microsoft") products, Windows NT 4.0 and Windows 2000. The government does not allege, however, that Mr. Genovese stole source code from

Microsoft. Rather, the government claims that he found and downloaded the code after it had been misappropriated from Microsoft and released onto the Internet by unknown third-party wrongdoers.

Under these circumstances, the Indictment must be dismissed because the EEA's definition section, 18 U.S.C. § 1839(3), is unconstitutionally vague as applied to Mr. Genovese, and is unconstitutionally overbroad on its face. First, Section 1839 defines a "trade secret" as information that is "not . . . generally known to . . . the public." In this case, the EEA's vague definition of "trade secret" left Mr. Genovese with no way of knowing whether the code he stumbled across on the Internet was "generally known" to the public by virtue of its presence in cyberspace. As a result, he had no way of knowing whether he was violating the EEA by allegedly downloading the code or offering to make it available to those who visited his website. Just as importantly, the law enforcement officers who arrested Mr. Genovese had no way of knowing whether he was violating the law by downloading portions of the source code and offering it for sale. This failure of statutory guidance renders the EEA unconstitutionally vague as applied to Mr. Genovese.

Second, Section 1839 states that information is a "trade secret" only if its owner "has taken reasonable measures to keep

such information secret." 18 U.S.C. § 1839(3)(A). Like "generally known to . . . the public," this definition left Mr. Genovese and law enforcement unable to determine whether the EEA outlawed the alleged conduct. For this reason, too, the EEA is unconstitutionally vague as applied to Mr. Genovese.

Third, since others have no better way of determining the EEA's contours than does Mr. Genovese, the EEA will necessarily chill substantial amounts of free expression: people must steer far clear of information that constitutes protected speech, simply because they are not certain whether the information constitutes a "trade secret" under the EEA. Because the EEA thereby chills too much protected speech relative to the legitimate sweep of the statute, it is unconstitutionally overbroad. As a result, the EEA is not only unenforceable against Mr. Genovese, it is invalid on its face.

FACTUAL BACKGROUND

At some time prior to February 12, 2004, portions of the source code for two Microsoft products – Windows NT 4.0 and Windows 2000 – were misappropriated.[1] See Declaration of Sean

[1] As set forth in the Complaint, "source code" is the human-readable code in which software developers write programs run by computers. Windows NT 4.0 and Windows 2000 are "operating systems." An operating system is the platform on which all other software applications run. Operating systems also control the allocation and usage of hardware resources such as memory,

Hecker ("Hecker Decl."), ¶ 3. It is not known who stole or leaked the portions of Microsoft's source code, or how it was obtained.[2] By February 12, 2004, however, the stolen code had been released onto the Internet, where it had instantly become available to anyone in the world with an Internet connection. Id., ¶¶ 3-4; Complaint ¶ 4(e). Indeed, by February 12, 2004, the code had been widely transmitted around the Internet in Internet chat rooms and elsewhere. See Hecker Decl. ¶ 3.

In the Complaint filed against Mr. Genovese, the government alleges that, on or about February 12, 2004, Mr. Genovese posted a message on his own website, called "illmob.org," indicating that he had obtained a copy of the stolen source code from the Internet and was willing to sell it. Complaint ¶ 5. The Complaint further alleges that later in February of 2004, an investigator hired by Microsoft obtained the stolen portions of source code from Mr. Genovese after contacting him by e-email and paying him $20 – an amount chosen by the investigator, not by Mr. Genovese – via PayPal, an online payment service. See Complaint

---

central processing unit time, disk space, and peripheral devices.

[2] News outlets have reported that the leak of the code has been traced to a computer used by the director of technology for Mainsoft, an Israeli software development company which had been hired by Microsoft four years earlier to investigate how certain key applications, including Internet Explorer, could be used by Linux-based operating systems. See Hecker Decl., ¶ 4.

¶¶ 6(a)-(d); Hecker Decl. ¶ 6. A second Microsoft investigator then repeated the process. See Complaint ¶ 6(d). Finally, the first Microsoft investigator provided instructions to an FBI agent on how to obtain the code from Mr. Genovese's website, which, the Complaint alleges, the FBI agent did in July of 2004. See Complaint ¶¶ 7-8.

On November 9, 2004, Mr. Genovese was arrested on a Complaint, which charged him with the unlawful distribution of trade secrets, in violation of Title 18, United States Code, Section 1832(a)(2), a provision of the EEA which criminalizes the knowing downloading or distribution of "trade secrets." On January 3, 2005, a grand jury returned an Indictment charging Mr. Genovese with the same offense. See Hecker Decl. ¶ 8.

As set forth below, the sole count of the Indictment must be dismissed because the EEA is unconstitutionally vague in at least two respects. In addition, the EEA is unconstitutionally overbroad in that it brings within its scope substantial amounts of protected free expression.

ARGUMENT

I. THE EEA IS UNCONSTITUTIONALLY VAGUE AS APPLIED TO THIS CASE BECAUSE ITS DEFINITION OF "TRADE SECRETS" FAILED TO PROVIDE MR. GENOVESE WITH FAIR NOTICE OF WHAT CONSTITUTED A CRIME.

Section 1832(a)(2) of the EEA makes it a crime for someone who intends to convert a "trade secret" to, among other things,

knowingly and without authorization copy, download, transmit or convey a "trade secret," if the person intends or knows that the offense will injure the "trade secret" owner. See 18 U.S.C. § 1832(a)(2). Section 1839(3) defines the term "trade secret":

> [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –
>
> > (A) the owner thereof has taken *reasonable measures* to keep such information secret; and
> >
> > (B) the information derives independent economic value, actual or potential, from not being *generally known to*, and not being readily ascertainable through proper means by, *the public*.

18 U.S.C. § 1839 (emphasis added).

In the circumstances of this case, the EEA's definition of "trade secret" is vague both with respect to its requirement that the owner take "reasonable measures" to keep the information secret and with respect the requirement that the information not be "generally known to . . . the public." Accordingly, the EEA failed to provide Mr. Genovese with fair notice of what conduct constituted a crime.

A. Due Process Requires Fair Notice of What Constitutes a Crime.

The Due Process Clause of the Fifth and Fourteenth Amendments requires a measure of specificity in criminal statutes. See, e.g., Giaccio v. Pennsylvania, 382 U.S. 399, 402-03 (1966). A criminal law that does not provide fair notice of what it forbids "violates the first essential of due process of law." Connally v. General Constr. Co., 269 U.S. 385, 391 (1926). "The vice of vagueness in criminal statutes is the treachery they conceal either in determining what persons are included or what acts are prohibited. Words which are vague or fluid may be as much of a trap for the innocent as the ancient laws of Caligula." United States v. Cardiff, 344 U.S. 174, 176 (1952) (citations omitted); See also Papachristou v. City of Jacksonville, 405 U.S. 156, 162 (1972) ("Living under a rule of law entails various suppositions, one of which is that '[all persons] are entitled to be informed as to what the State commands or forbids.'") (quoting Lanzetta v. New Jersey, 306 U.S. 451, 453 (1939)).

A law is void for vagueness if it suffers from either of the following defects: first, it "may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits"; alternatively, it "may authorize and even encourage arbitrary and discriminatory enforcement." Chicago v.

Morales, 527 U.S. 41, 56 (1999) (citing Kolender v. Lawson, 461 U.S. 352, 357 (1983) (establishing the current version of the two-prong test)); see also United States v. Rybicki, 354 F.3d 124, 129 (2d Cir. 2003). In the absence of First Amendment implications (discussed in Section II, infra), a void-for-vagueness challenge is as-applied; the statute is assessed for vagueness only "in light of the specific facts of the case at hand and not with regard to [its] facial validity." Rybicki, 354 F.3d at 129 (quoting United States v. Nadi, 996 F.2d 548, 550 (2d Cir. 1993), cert. denied, 510 U.S. 933 (1993)). "One whose conduct is clearly proscribed by the statute cannot successfully challenge it for vagueness." Id.

Finally, "legislation creating 'new' crimes (which does not generically tend to be unclear, but is likely to represent affirmative legislative intrusion into realms previously left to individual freedom) is particularly vulnerable to vagueness attack." United States v. Hsu, 40 F. Supp. 2d 623, 626 (E.D. Pa. 1999) (quoting Anthony G. Amsterdam, The Void-for-Vagueness Doctrine in the Supreme Court, 109 U. Pa. L. Rev. 67, 84 (1960)). As the Hsu court noted, the EEA is such "new crime" legislation, "criminalizing, as it does, conduct that heretofore was thought best left to the civil law of unfair competition and cognate jurisprudence." Hsu, 40 F. Supp. 2d at 626.

B. The EEA's "Generally Known To . . . The Public" Definition Is Unconstitutionally Vague.

In this case, it is undisputed that Mr. Genovese did not engage in first-order trade secret theft – that is, he did not somehow break into Microsoft's systems and take any part of the source code for any Microsoft product. Instead, the government alleges that (1) unknown parties stole or otherwise obtained at least parts of the source code for the two Microsoft products and released them onto the Internet, where they became accessible to anyone with an Internet connection; (2) Mr. Genovese found the stolen code on the Internet and downloaded it to his computer; and (3) Mr. Genovese placed a message on his Web site offering to sell the code that he had downloaded from the Internet. As a result of these actions, the government has charged Mr. Genovese with violating the EEA by downloading and transmitting information that, among other things, was not "generally known to . . . the public." 18 U.S.C. § 1839(3)(B).[3]

1. The "generally known to . . . the public" phrase failed to provide reasonable notice to Mr. Genovese.

As set forth above, a statute is impermissibly vague if it

[3] This case is hardly a typical EEA prosecution. Indeed, we have not been able to identify any other reported cases reflecting EEA prosecutions brought against defendants who were not alleged to have been directly involved in the initial theft of the information purportedly constituting the "trade secret."

"fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits." Morales, 527 U.S. at 56. In other words, the statute must provide individuals with "relatively clear guidelines as to prohibited conduct," in order to pass the first prong of the void-for-vagueness test. Posters 'N' Things v. United States, 511 U.S. 513, 525 (1994). This test "is essentially a definitional requirement: a penal statute must speak for itself so that a lay person can understand the prohibition. It is not enough to say that judges can intuit the scope of the prohibition if [defendant] could not." United States v. Hand, 286 F.3d 92, 104 (2d Cir. 2002).

The EEA provided no such guidance to Mr. Genovese. By the time he allegedly downloaded portions of the source code for Windows NT 4.0 and Windows 2000, the code had already been leaked onto the Internet, where it was available to anyone in the world with Internet access. Indeed, numerous people had in fact obtained the code immediately after its release. Hecker Decl. ¶ 3. Once the code was available to anyone with Internet access, and, in fact, obtained by an unknown number of people, it is, at best, unclear whether the code were "generally known" to the

public.[4] But the statute offers no criteria for determining whether such a broad release of the information made it "generally known" to the public. Must hundreds of people know? Thousands? More? The EEA provides no "relatively clear" guidance. As a result, Mr. Genovese had no way of knowing whether the material he was downloading was a "trade secret." Therefore, the EEA is unconstitutionally vague as applied to him.

In United States v. Hsu, the court considered a vagueness challenge to precisely this aspect of the EEA's definition of what constitutes a "trade secret." The court noted that "what is 'generally known' . . . about ideas, concepts, and technology is constantly evolving in the modern age." Hsu, 40 F. Supp. 2d at 630. The court added that the meaning of "public" was unclear, as was the effect of Internet availability of the information in question. Id. The court stated that it was "much troubled by the EEA's vaporous terms." Id.

The Hsu court ultimately declined to hold the EEA void for vagueness because the Hsu defendants were fully aware that the

---

[4] Indeed, it is difficult to imagine how a "trade secret" could remain a "secret" after it has been widely disseminated over the Internet. See DVD Copy Control Assoc. v. Bunner, 116 Cal. App. 4th 241, 251-52, 10 Cal. Rptr. 3d 185, 192-93 (Cal. Ct. App. 2004) (discussing whether "secrecy requirement" can be maintained after "[w]idespread, anonymous publication of information over the Internet").

information they allegedly appropriated was not generally known: they had been told beforehand that their actions were illegal; they knew the information they sought was not publicly available; and they knew the only way they could acquire it was through a corrupt company employee. Hsu, 40 F. Supp. 2d at 631. In the face of these damning facts, the court decided to "put aside our considerable disquiet about the EEA's language" and deny the as-applied vagueness challenge. Id.

The facts of the Hsu case, however, are easily distinguished. Mr. Genovese obtained the information from the Internet, not from a corrupt Microsoft employee or licensee. As a result, he had every reason to believe the code had become publicly available. Furthermore, unlike the Hsu defendants, there is no allegation that Mr. Genovese had been warned that it would be a crime for him to post the source code on his website and offer to distribute it to even more people. The lack of a warning is critical to a void-for-vagueness analysis, which is driven by the due-process mandate that individuals be given notice that their conduct might violate the law. See Perez v. Hoblock, 368 F.3d 166, 177 (2d Cir. 2004) (because vagueness doctrine is based on the idea of fair notice, fact that defendant received explicit notice that his conduct was illegal undermined challenge); Advance Pharm. v. United States, 391 F.3d 377, 397

(2d Cir. 2004) (defendants' as-applied vagueness challenge failed because DEA agents had clarified law for them before incidents in question). Given the Hsu court's extreme discomfort with the EEA's vague terms, it seems likely it would have decided the case differently if the instant facts were before the court. See Robin D. Ryan, The Criminalization of Trade Secret Theft Under the Economic Espionage Act of 1996, 25 Dayton L. Rev. 243, 255 (2000) ("Because the defendant in Hsu knew, or at a minimum believed, that he was stealing trade secrets, his indictment is well-founded; however, under different circumstances, the EEA is vulnerable to the vagueness attack.").

2. The "generally known to . . . the public" phrase encourages arbitrary enforcement of the statute.

A statute can also be impermissibly vague if it "authorize[s] and even encourage[s] arbitrary and discriminatory enforcement." Morales, 527 U.S. at 56. Although this second prong of the void-for-vagueness test is independent of the fair notice requirement, the two are closely related. As the Supreme Court made clear in Posters 'N' Things, both prongs are driven by the requirement that a statute provide "relatively clear criteria" for determining what is prohibited; those "clear criteria" serve both to provide notice to the public (prong one) and to cabin law enforcement discretion, preventing arbitrary

arrests (prong two). See Posters 'N' Things, 513 U.S. at 525 (upholding statute because list of prohibited items "provides individuals and law enforcement officers with relatively clear guidelines as to prohibited conduct."); see also United States v. Venturella, 391 F.3d 120, 133 (2nd Cir. 2004) ("vagueness doctrine is a "manifestation of the fair warning requirement"); Hand, 286 F.3d at 101 ("A criminal statute is void for vagueness if it fails to . . . channel the discretion of the prosecution.").

In this case, the same failure that renders the "generally known" language invalid under the notice prong also causes it to flunk the arbitrary enforcement prong. The FBI agents enlisted by Microsoft to investigate and arrest Mr. Genovese had no better way of deciding whether the Microsoft source code was "generally known" to the public -- and thus outside the EEA's ambit -- than Mr. Genovese did. The leaked source code appeared all over the Internet, not just on Mr. Genovese's website. In how many places did the code need to appear before the information was "generally known," and thus no longer a "trade secret" under the EEA? The statute provides no guidance whatsoever, and it therefore "may authorize and even encourage arbitrary and discriminatory enforcement." Morales, 527 U.S. at 56.

The Supreme Court addressed a comparable situation in Kolender v. Lawson. There, the California statute at issue required persons wandering the streets to provide "credible and reliable" identification when requested by a police officer. The phrase "credible and reliable" was undefined. The Court struck down the statute, explaining that its vague phrasing improperly left the burden on law enforcement officials to decide, without guidance, when the law had been violated:

> Section 647(e) . . . contains no standard for determining what a suspect has to do in order to satisfy the requirement to provide a "credible and reliable" identification. As such, the statute vests virtually complete discretion in the hands of the police to determine whether the suspect has satisfied the statute and must be permitted to go on his way in the absence of probable cause to arrest.

Kolender, 461 U.S. at 358. The provision of the "trade secrets" definition at issue here, like the statute in Kolender, vested "virtually complete discretion" in the FBI agents enlisted by Microsoft to decide whether the information Mr. Genovese had downloaded and offered for sale was "generally known" to the public. The EEA gave them no guidance in making that decision, and therefore it is unconstitutionally vague.

C. The EEA's "Reasonable Measures" Phrase Is Also Unconstitutionally Vague.

In order for information to constitute a "trade secret" under the EEA, its owner must have taken "reasonable measures" to

keep it a secret. See 18 U.S.C. § 1839(3)(A). As a result, Mr. Genovese only could have violated the EEA if Microsoft took "reasonable measures" to protect the privacy of the source code for Windows NT 4.0 and Windows 2000. But this requirement also fails a vagueness challenge.

1. The "reasonable measures" phrase failed to provide Mr. Genovese notice as to whether he was violating the law.

The EEA fails to provide any meaningful guidance about what would constitute "reasonable measures" for a purported trade secret holder to take in order to keep maintain secrecy. And the Act provides no objective criteria by which to judge the "reasonableness" of such preventative measures. Even an alleged first-order thief – e.g., one who actually broke into Microsoft's offices, accessed its computer systems, and stole the code – may or may not have been able to ascertain whether the steps Microsoft had taken to protect its code constituted "reasonable measures" and, thus, whether the information would be deemed a "trade secret" under the EEA. See United States v. L. Cohen Grocery Co., 255 U.S. 81, 89 (1921) (holding that federal statute which made it unlawful "to make any unjust or *unreasonable* rate in handling or dealing in or with any necessaries" failed to provide fair notice of what was prohibited and was thus void for vagueness) (emphasis added).

For instance, if a company insider with intimate knowledge of Microsoft's security infrastructure had taken the source code, any vagueness problems would probably not rise to a level of constitutional concern. The same might or might not be said of an industry insider – perhaps a security consultant – who knew something about Microsoft's security practices, as well of those common to the industry. Indeed, there may be a spectrum of defendants whose knowledge of a company's security measures outweighs any concern about the potential vagueness of this aspect of the EEA's trade secrets definition.

But under the circumstances present here, faced with a defendant who is an alleged second-order trade secrets thief who found the stolen code on the Internet, applying the "reasonable measures" language borders on the absurd. Mr. Genovese was in no position to make a determination about whether Microsoft took any measures to protect the secrecy of its source code, let alone whether those measures were "reasonable."

The "reasonable measures" requirement was imported into the EEA from the common law. See Andrew Beckerman-Rodau, Trade Secrets: The New Risks to Trade Secrets Posed by Computerization, 28 Rutgers Comp. & Tech. L.J. 227, 240-41 (2002). Under the common law, courts considered the following in determining whether a trade secret owner's privacy-protection measures were

reasonable: (1) whether the owner complied with standard industry practice, (2) whether the owner invested adequate resources to insure secrecy, (3) whether the owner advised employees and others that a trade secret existed, (4) whether the owner limited knowledge of the trade secret to a need-to-know basis, and (5) whether the owner required employees to sign non-disclosure agreements prior to disclosing the trade secret to them. Id., at 240-41. For purposes of this as-applied challenge these questions all have one common attribute: Mr. Genovese could not have answered them as they related to Microsoft's treatment of its source code. As a result, the EEA did not afford him with a "reasonable opportunity to understand" what conduct the law prohibited, and the "reasonable measures" definition is unconstitutionally vague.

2. The "reasonable measures" phrase encourages arbitrary enforcement of the statute.

Because the EEA provides no objective criteria by which to judge the "reasonableness" of preventative measures, the FBI agents enlisted by Microsoft to investigate Mr. Genovese were similarly hamstrung in their ability to determine whether Microsoft's security measures were sufficient. The EEA thus violates prong two of the void-for-vagueness test, which requires that a statute gives law enforcement officers "relatively clear

guidelines as to prohibited conduct," Posters 'N' Things, 513 U.S. at 525, so as to prevent arbitrary or discriminatory enforcement. See Franza v. Carey, 518 F. Supp. 324 (S.D.N.Y. 1981) (holding void for vagueness a drug paraphernalia law which prohibited sale of items if a "reasonable person" would know the drug-related purpose of the item). As one commentator has noted about the EEA, the "reasonable measures" phrase "exudes vagueness" because it "simply does not indicate to courts whether the measures taken to keep information secret should be guided by standards of the scientific community, the judicial community, or the public." Ryan, 25 Dayton L. Rev. at 256. On this basis, too, the EEA is unconstitutional as applied to Mr. Genovese.

D. Other Well-Established Due Process Considerations Reinforce The Conclusion That The EEA Is Vague As Applied To Mr. Genovese.

The degree of statutory vagueness tolerated by the Constitution, and the relative importance of fair notice, depend in part on the nature of the statute at issue. See Hoffman Estates v. Flipside, Hoffman Estates, 455 U.S. 489, 498 (1982). Specifically, the Supreme Court has "expressed greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe," id., at 498-499.

Here, the EEA's heavy criminal penalties argue strongly in favor of a vagueness finding. As the Court stated in Hoffman Estates, the void-for-vagueness test is more exacting in the criminal context for the obvious reason that the consequences of vagueness are more severe. In this case, Mr. Genovese faces up to ten years in federal prison if he is convicted of this offense. Given that the Supreme Court saw fit to use a "relatively strict" vagueness test even where the statute in question was only "quasi-criminal" and violations resulted only in fines, see Hoffman Estates, 455 U.S. at 500, the statute should receive even less leeway here.[5]

For all of these reasons, this Court should hold that the EEA is unconstitutionally vague as applied to the circumstances of Mr. Genovese's case.

[5] The Supreme Court has "recognized that a scienter requirement may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed." Hoffman Estates, 455 U.S. at 499 (internal citations omitted). And the EEA does require both that the defendant know that the information appropriated is a "trade secret," and that he have an intent to convert the "trade secret" for the benefit of someone other than the owner. See 18 U.S.C. § 1832(a). But these scienter elements do nothing to mitigate the vagueness problems in this context. The EEA's vague definition of "trade secrets" left Mr. Genovese unable to know whether the information he obtained was a "trade secret."

II. THE EEA IS UNCONSTITUTIONALLY OVERBROAD BECAUSE THE VAGUENESS OF ITS TRADE SECRETS DEFINITION WILL CHILL TOO MUCH PROTECTED SPEECH

A. The Overbreadth Doctrine Invalidates Statutes Which Chill Too Much Protected Speech Relative to the Legitimate Scope of the Statute.

The government may restrict certain types of speech and expressive conduct, but laws imposing such restrictions must be narrowly tailored to the harm the government legitimately seeks to ameliorate. See, e.g., Gooding v. Wilson, 405 U.S. 518, 520-21 (1972) (requiring "narrow specificity" in such laws). When a statute has the potential to punish not only the unprotected speech at which it is aimed but also substantial amounts of protected speech, the law may be struck down as unconstitutionally overbroad. See generally Broadrick v. Oklahoma, 413 U.S. 601 (1973).

The doctrine of First Amendment overbreadth also constitutes an exception to the standing rule, which otherwise prevents litigants from raising facial challenges to a statute's constitutionality unless they can show that no set of circumstances exists under which the statute would be valid. See Lerman v. Board of Elections, 232 F.3d 135, 144 (2d Cir. 2000). As the Second Circuit has recognized, an individual charged under an overly broad statute can raise a facial challenge to the constitutionality of the statute even if he cannot demonstrate

that it chilled his own First Amendment rights. See Lebron v. AMTRAK, 69 F.3d 650, 659 (2d Cir. 1995) (citing Broadrick, 413 U.S. at 612). Litigants "are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from constitutionally protected speech or expression." Broadrick, 413 U.S. at 612.

Courts permit such facial challenges out of "concern that the threat of enforcement of an overbroad law may deter or 'chill' constitutionally protected speech -- especially when the overbroad statute imposes criminal sanctions." Virginia v. Hicks, 539 U.S. 113, 119 (2003) (collecting cases). The Supreme Court has justified the overbreadth doctrine on the ground that "[m]any persons, rather than undertake the considerable burden (and sometimes risk) of vindicating their rights through case-by-case litigation, will choose simply to abstain from protected speech -- harming not only themselves but society as a whole, which is deprived of an uninhibited marketplace of ideas." Id. (internal citations omitted).

Under the overbreadth doctrine, a facial challenge "need only 'demonstrate a substantial risk' that application of the provision will lead to the suppression of speech." Lerman, 232

F.3d 135 at 144 (quoting National Endowment for the Arts v. Finley, 524 U.S. 569, 580 (1998)). This "substantial risk" may be apparent from the plain language of a statute; alternatively, a statute's vagueness may create the overbreadth problem by giving law enforcement discretion to make arrests for a wide range of speech, some of which is protected and some of which is not. See Houston v. Hill, 482 U.S. 452, 466 (1987) (ordinance overbroad because it "accords the police unconstitutional discretion in enforcement").

Laws that suppress or proscribe substantial amounts of constitutionally protected speech may be held facially invalid even if they also have legitimate applications. Hill, 482 U.S. at 459. The Supreme Court has framed the test as follows: If a law "punishes a substantial amount of protected speech or conduct, judged in relation to the statute's plainly legitimate sweep," the law is invalid until and unless a limiting construction or partial invalidation so narrows it as to remove the threat. Hicks, 539 U.S. at 119 (quoting Broadrick, 413 U.S. at 615). In other words, where a statute's application to protected speech is substantial, "not only in an absolute sense, but also relative to the scope of the law's plainly legitimate

applications," the law must either be invalidated or judicially narrowed. Hicks, 539 U.S. at 120.[6]

B. The EEA Potentially Applies to Substantial Amounts of Protected Speech

The Second Circuit has already held that computer code constitutes protected "speech" for purposes of the First Amendment. See Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445 (2d Cir. 2001) ("Communication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code."). Indeed, the universe of protected speech is vast. As the Second Circuit has explained:

> Some would confine First Amendment protection to political speech. . . . Whatever might be the merits of these and other approaches, the law has not been so limited. Even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection. . . . Thus, for example, courts have subjected to First Amendment

---

[6] The analysis of whether a law is unconstitutionally overbroad overlaps substantially with the "intermediate scrutiny" that the Supreme Court applies to "content neutral" speech regulations. The EEA is "content neutral" because it "serves purposes unrelated to the content of expression." Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989). Under intermediate scrutiny a regulation must (1) "promote a substantial government interest that would be achieved less effectively absent the regulation," and (2) not "burden substantially more speech than is necessary to further the government's legitimate interests." Ward, 491 U.S. at 799. The EEA would fail intermediate scrutiny for same reasons that it is unconstitutionally overbroad. See Sections II.B. and II.C., infra.

> scrutiny restrictions on the dissemination of technical scientific information and scientific research, and attempts to regulate the publication of instructions. . . . Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer. . . . [T]he fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions "speech" for purposes of the First Amendment.

Id., 273 F.3d at 446-447 (internal citations omitted).

There can thus be no doubt that the Microsoft source code alleged to have been downloaded and offered for sale by Mr. Genovese constitutes protected speech. So too does each of the types of information identified by the EEA as a potential "trade secret." See 18 U.S.C. § 1839(3) (including "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."). Each of these items constitutes protected speech, because each "convey[s] . . . information." Id., 273 F.3d at 447. See also Roth v. United States, 354 U.S. 476, 484 (1957) (First Amendment embraces "all

ideas having even the slightest redeeming social importance," including the "advancement of truth, science, morality, and arts in general"); Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 763 (1976) (prescription drug price information is speech because a consumer's interest in "the free flow of commercial information" may be "keener by far" than "his interest in the day's most urgent political debate"). In short, the EEA potentially criminalizes a substantial amount of otherwise protected First Amendment speech.

C. The EEA's Vagueness Chills Far More Protected Speech Than Can Be Justified By Its Legitimate Scope.

Here, because of the vagueness of the EEA's definition of the term "trade secret," discussed in Section I, supra, the EEA effectively burdens substantially more speech than is necessary to achieve the Government's goal of preventing the theft of actual trade secrets. Indeed, because the definition of "trade secret" is so vague, it is nearly impossible for anyone obtaining quasi-public information -- whether on the Internet or from a journalistic source, for example -- to determine whether the information could be deemed to constitute a "trade secret," the further dissemination of which would be a crime under the EEA. As a result, individuals in journalism, technology, and

information services must avoid disseminating or trading in such information, even if it is not truly a trade secret.

There are a number of ways that the EEA could be more narrowly tailored to the Government's aims while burdening substantially less protected speech. First, the legislation could exempt from its scope otherwise lawful activity conducted by a person whose intent is to engage in criticism, comment, news reporting, teaching, scholarship, or research. An analogy can be found in the context of the federal Copyright Act, which exempts from its scope such "fair uses" of copyrighted material. See 17 U.S.C. § 107 (setting forth four factors to be considered in determining whether use is a "fair use"). Notably, the EEA already exempts from its scope both the activities of governmental entities, see 18 U.S.C. § 1833(1), and certain forms of whistle-blowing, see 18 U.S.C. § 1833(2).

Second, the legislation could be re-drafted to eliminate some of the vagueness concerns outlined in Section I, supra. The EEA definition of "trade secrets" could clarify that information that has already been distributed in public fora, such as the Internet, loses its protected status as a "trade secret." The definition also could include a list of objective criteria by which one could measure the "reasonableness" of a company's preventative measures, such as those found in the common law.

As written, however, this Court should find that the EEA is unconstitutionally overbroad, because it burdens "substantially more speech than is necessary to further the government's legitimate interests" in preventing the theft of genuine trade secrets. The statute's very existence "may cause others not before the court to refrain from constitutionally protected speech or expression." Broadrick, 413 U.S. at 612. When that occurs, such individuals are "harming not only themselves but society as a whole, which is deprived of an uninhibited marketplace of ideas." Hicks, 539 U.S. at 119.

The EEA's harsh criminal penalties, which include the possibility of up to 10 years in prison, also counsel in favor of a finding that the EEA is unconstitutionally overbroad. As the Second Circuit has stated: "[I]t bears emphasizing that the penalty to be imposed is relevant in determining whether demonstrable overbreadth is substantial. Although the fact that a criminal prohibition is involved does not . . . a priori warrant a finding of substantial overbreadth, it does appreciably shrink the amount of overbreadth we will find constitutionally tolerable, particularly when the penalty is severe." Rybicki, 354 F.3d at 130 n.2 (quoting Massachusetts v. Oakes, 491 U.S. 576, 595-96 (1989)).

CONCLUSION

The EEA is unconstitutionally vague as applied to Mr. Genovese's case because it failed to provide him, or the FBI agents who investigated him, with intelligible standards for determining whether he committed a crime by allegedly downloading or offering to sell the Microsoft source code he found on the Internet. Furthermore, the statute is facially unconstitutional because the vagueness of its trade secret definition necessarily will chill a substantial amount of protected speech, even when judged in relation to its legitimate sweep. For these reasons, the Court should dismiss the Indictment.

Dated: New York, New York
March 16, 2005

Respectfully Submitted,
LEONARD F. JOY, ESQ.
The Legal Aid Society
Federal Defender Division

BY: _____
SEAN HECKER, ESQ.
Attorney for
WILLIAM GENOVESE